State of DMARC

Tim Draegen
tim@dmarcian.com

21 April 2015

About The Presenter

- mid/late-80’s: Apple IIe programming, FidoNet
- early 90’s: x86 programming (fractals!)
- mid 90’s to 2000: intern->employee @ ཇོ
- 2000-2004: three 1-year stints at startups (BSD)
- 2004-2008: IronPort/Cisco (email security)
- 2009-2010: Nominum (large DNS software)
- 2010-2012: Co-founded email intel company
- 2013: Message Bus (VP Marketing!)
- 2014+:
    - dmarcian.com
    - co-Chair of IETF DMARC Working Group

Our Roadmap

- Email, Standards, and DMARC
- What is DMARC accomplishing?
- Notes on deploying DMARC

EMA

WEB

SOCIAL

EVERYTHING ELSE ONLINE

IL

* Pretty close to scale

Where do standards come from?

Theory of Practice

- Big party +
- Great ideas +
- Spirited debate =
  - Specification

- Things get built +
- Easy interoperability =
  - New standard!

Practice of Theory

- Big problem +
- Installed base +
- Entrenched interests =
  - Problem space

- Begging/Coercion +
- Layer cake of hacks +
- Something that finally works =
  - New standard!

Email Standards

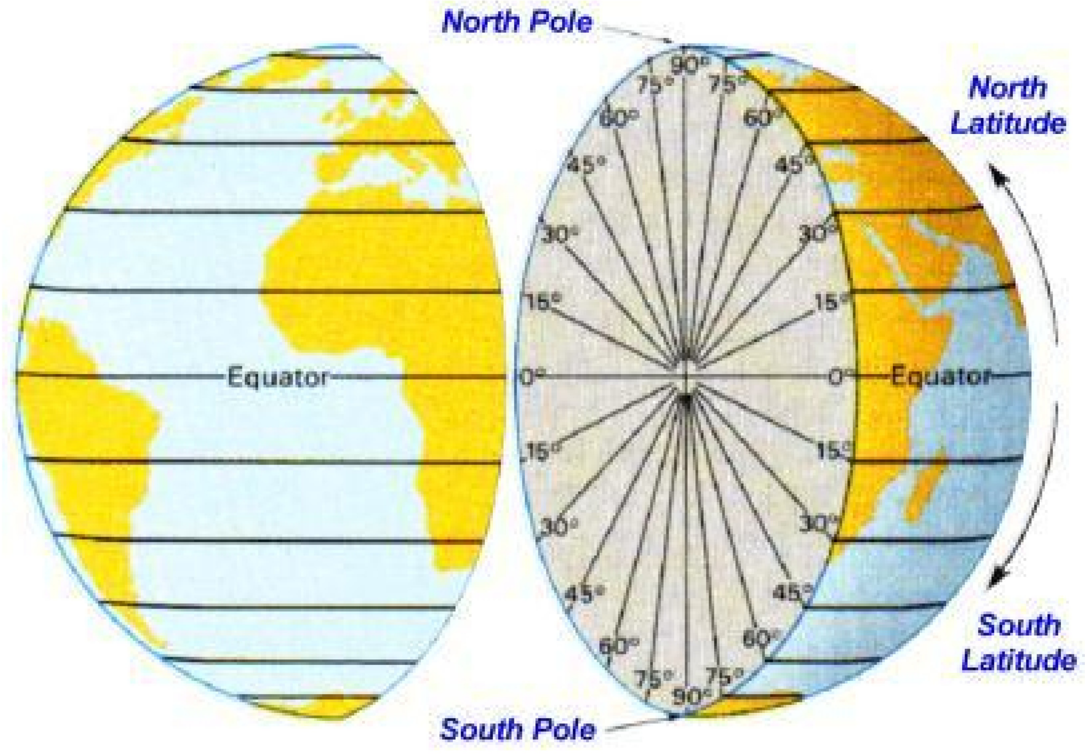
- RFC 5598 Internet Mail Architecture, July 2009
  - “Over its thirty-five-year history..”
- RFC 561 Standardizing Network Mail Headers, September 1973
  - “One of the deficiences[sic] of the current FTP mail protocol is that it makes no provision for the explicit specification of such header information as author, title, and date. Many systems send that information, but each in a different format. One fairly serious result of this lack of standardization is that it's next to impossible for a system or user program to intelligently process incoming mail.”

Email Still Big

- Every component of Internet Mail Architecture represents an industry.
- Lots of components! Lots of industries.
- Lots of industry *communities*.
  - *..but no single mega community of communities*
- No one works on the whole thing.*

* but everyone can have an opinion!

If the problem is too big…

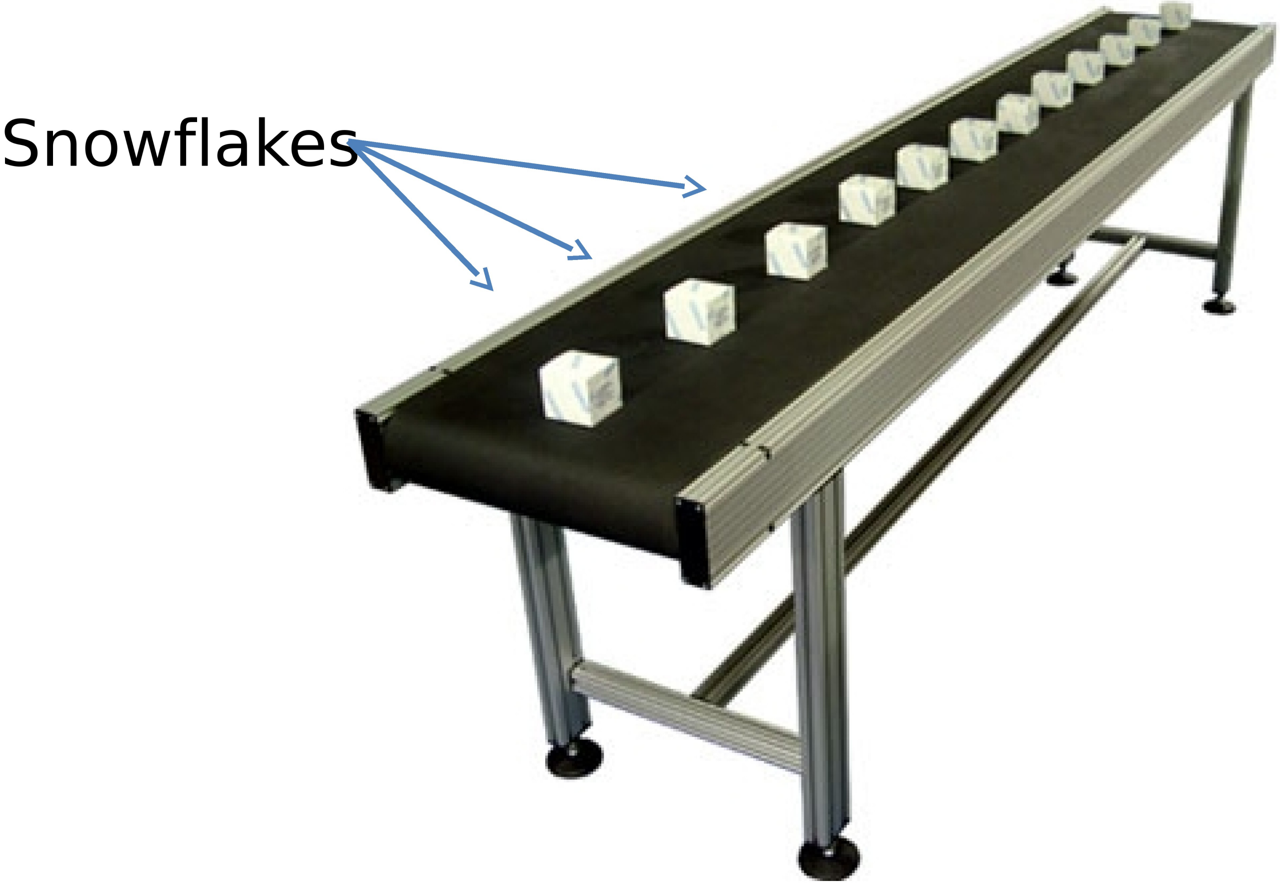


cut it in half!

From the Point of View of an Email Receiver

WITH WHAT I'M SEEING HERE AND THE DNA TESTS, SEEMS LIKE WE GOT OURSELVES A GENUINE E-MAIL!
ISP LAB
SPAM
NOT SPAM
NOT SPAM, BUT LETS LABEL IT SPAM ANYWAY
EMAIL AUTHENTICATION

From the Point of View of an Email Receiver



Snowflakes

Every email is unique..

..and every sender wants theirs delivered NOW.

An Insidious Situation

Blocking legitimate email is really bad:

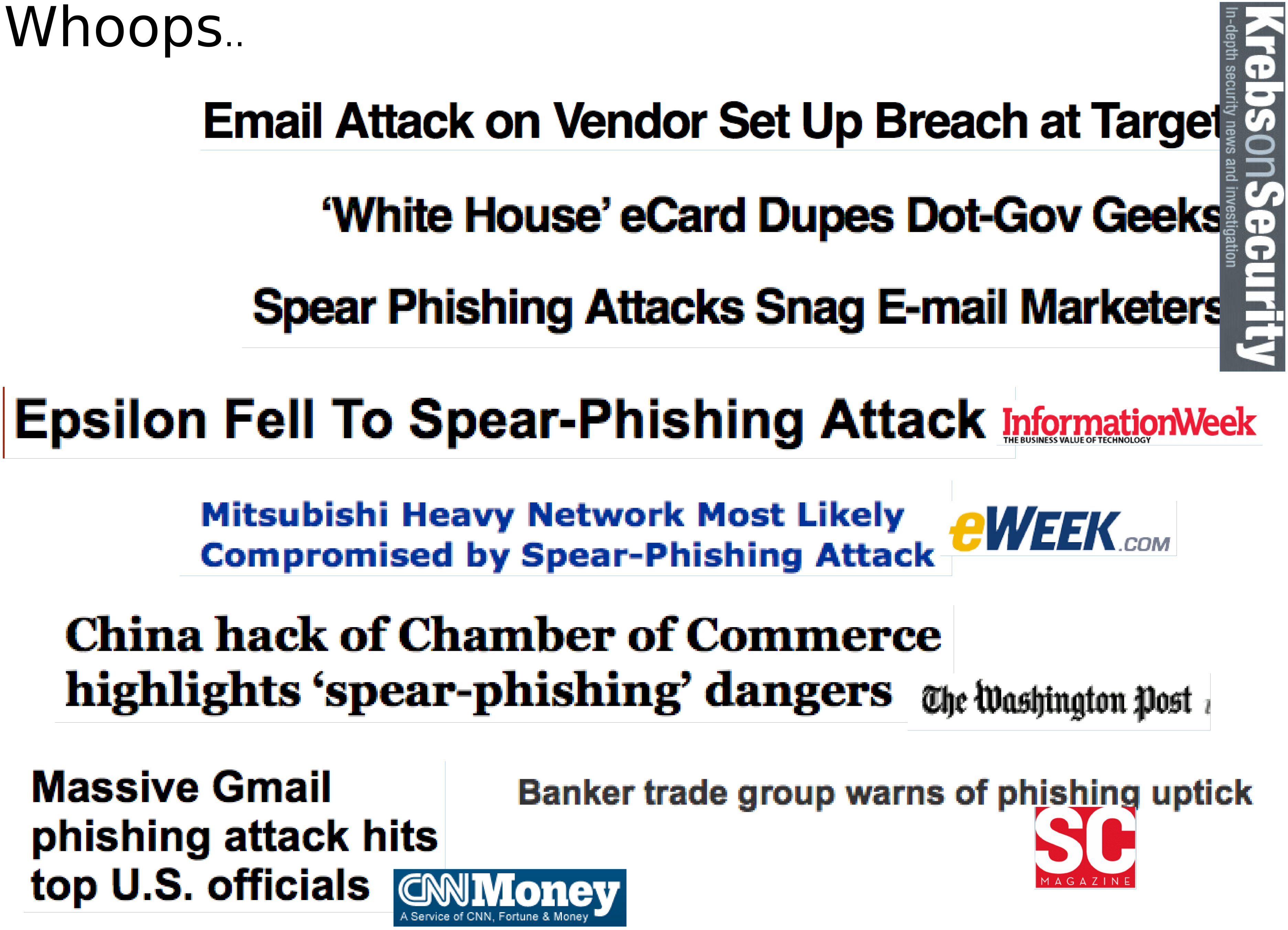
- Support costs = ouch!
- Heads might roll depending on recipient
- In ISP-world, users go somewhere else

There is a terribly thin line between the sloppiest legitimate email and expertly crafted phishing.

∴ *the most effective fraud gets through..*

..and criminals are incentivized to get better!

Whoops..



Email Attack on Vendor Set Up Breach at Target

'White House' eCard Dupes Dot-Gov Geeks

Spear Phishing Attacks Snag E-mail Marketers

KrebsonSecurity
In-depth security news and investigation

Epsilon Fell To Spear-Phishing Attack

InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

Mitsubishi Heavy Network Most Likely Compromised by Spear-Phishing Attack

eWEEK.COM

China hack of Chamber of Commerce highlights 'spear-phishing' dangers

The Washington Post

Massive Gmail phishing attack hits top U.S. officials

Banker trade group warns of phishing uptick

The root of it all

- Anyone can send whatever email they want..

- .. including pretending they’re someone they’re not.

- How does one make email easy to identify?
  - How can we tag snowflakes with IDs?

An Echo From The Past?

- RFC 561 Standardizing Network Mail Headers, September 1973
  - “Many systems send that information, but each in a different format. One fairly serious result of this lack of standardization is that it's next to impossible for a system or user program to ~~intelligently process incoming mail~~ determine if mail is legitimate.”

The Journey to Easy Email ID

Time

Sender Adoption

Receiver Adoption

2003-2006: building blocks (SPF, DomainKeys, DKIM)

"I've heard this helps"

Nice to have as anti-spam input, not reliable

2007-2009: prototype authenticated email model

PayPal innovates, Financial Services publishes recommendations

Yahoo & Gmail reject fake PayPal email, other big providers take note

2010-2011: make it work at internet scale

PayPal funds/organizes effort to standardize the model

Big webmail providers commit to support and implement

2012-2013: early adopters

Senders with fraud and clean infrastructures deploy

Big consumer mailboxes and those that can roll their own deploy

2014-2015: not just for security/anti-phishing! Make it work everywhere.

DMARC at the IETF

- Base spec submitted to IETF (March 2013)

- Working Group chartered to work on interoperability issues between DMARC and *indirect email flows.* (Aug 2014)

- Base spec RFC 7489 (March 2015)
  - *INFORMATIONAL*

- http://trac.tools.ietf.org/wg/dmarc/trac/wiki

Standards are nice, but..

What is dmarc accomplishing?

First: DMARC Features

DMARC

- **Overlay** – Leverages SPF and DKIM as authentication mechanisms
  - □ Describes how to deploy SPF and DKIM… consistency
- **Visibility** – Describes new feedback mechanism
  - □ Gives senders visibility into how receivers process their email
- **Protection** – Senders can declare how to process auth-failing email
  - □ Specifies a DNS-based policy model that incorporating SPF + DKIM results

SPF

*Path-based (*RFC 4408)
Authorized servers published via simple DNS record
Very low deployment cost
Forwarding breaks SPF

Is the messenger (server) permitted?

DKIM

Signature-based (RFC 6376)
Requires cryptographic operation by email gateways
Public keys published via DNS
Can survive forwarding

Is the signature authentic?

Identifiers in SMTP Conversation

Outbound Email Server
(smtp.sample.net)

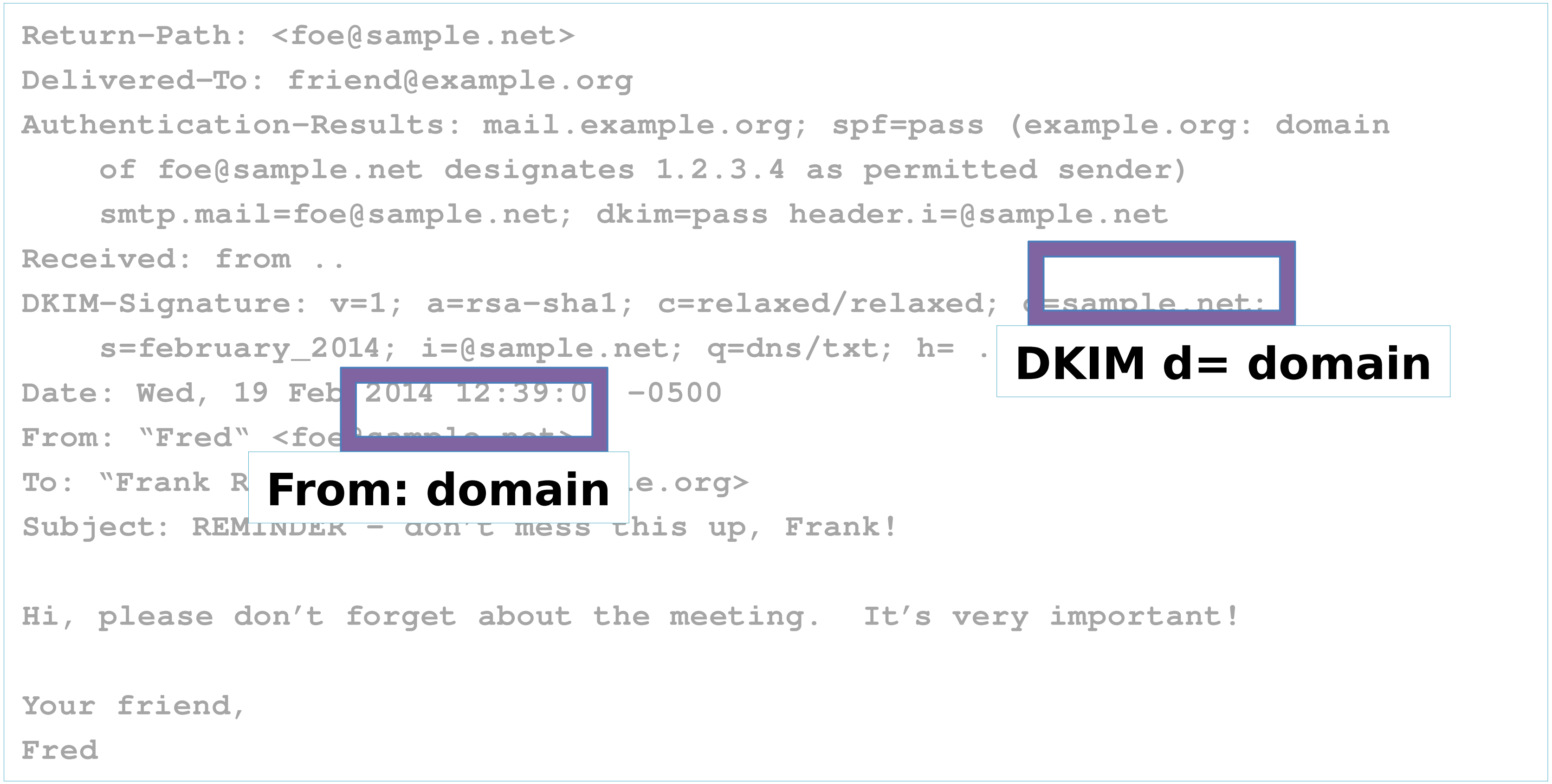
Receiving Server
(mail.example.org)

```
HELO smtp.sample.net
                                         250 mail.example.org
MAIL FROM: <foe@sample.net>
                             250 sender <foe@sample.net> ok
RCPT TO: <fr                  rg>
                    250 recipient <friend@example.org> ok
DATA
                                              354 go ahead
(email content here)
                          250 ok: Message 17763873 accepted
QUIT
                                         221 mail.example.org
```

Envelope domain

(email now subject to anti-spam and then delivery)

Identifiers In Content



```
Return-Path: <foe@sample.net>
Delivered-To: friend@example.org
Authentication-Results: mail.example.org; spf=pass (example.org: domain
    of foe@sample.net designates 1.2.3.4 as permitted sender)
    smtp.mail=foe@sample.net; dkim=pass header.i=@sample.net
Received: from ..
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; d=sample.net;
    s=february_2014; i=@sample.net; q=dns/txt; h= .
Date: Wed, 19 Feb 2014 12:39:0  -0500
From: “Fred“ <foe@sample.net>
To: “Frank R                   e.org>
Subject: REMINDER - don’t mess this up, Frank!

Hi, please don’t forget about the meeting.  It’s very important!

Your friend,
Fred
```

DKIM d= domain

From: domain

Accomplishments

- New visibility into how email domain is used
  - bonus: insight into robustness of SPF/DKIM
- Serious exact domain anti-phishing
  - bonus: more scrutiny of non-DMARC email
- Simplified delivery
  - bonus: simplified filtering!
- Domain reputation
  - *big shift in what is important in email world*

SIDEBAR: IPv4 and Email

- IPv4 address has long been most stable thing related to email.

- IPv4 reputation is first line of email defense.
  - *IPv6 ruins everything! Too many numbers!*

- DMARC’s stable domain-level identifiers is the “upgrade path” from IPv4 reputation

Not Accomplished YET

- DMARC’s stable domain-level identifiers enable MUAs to finally get better.

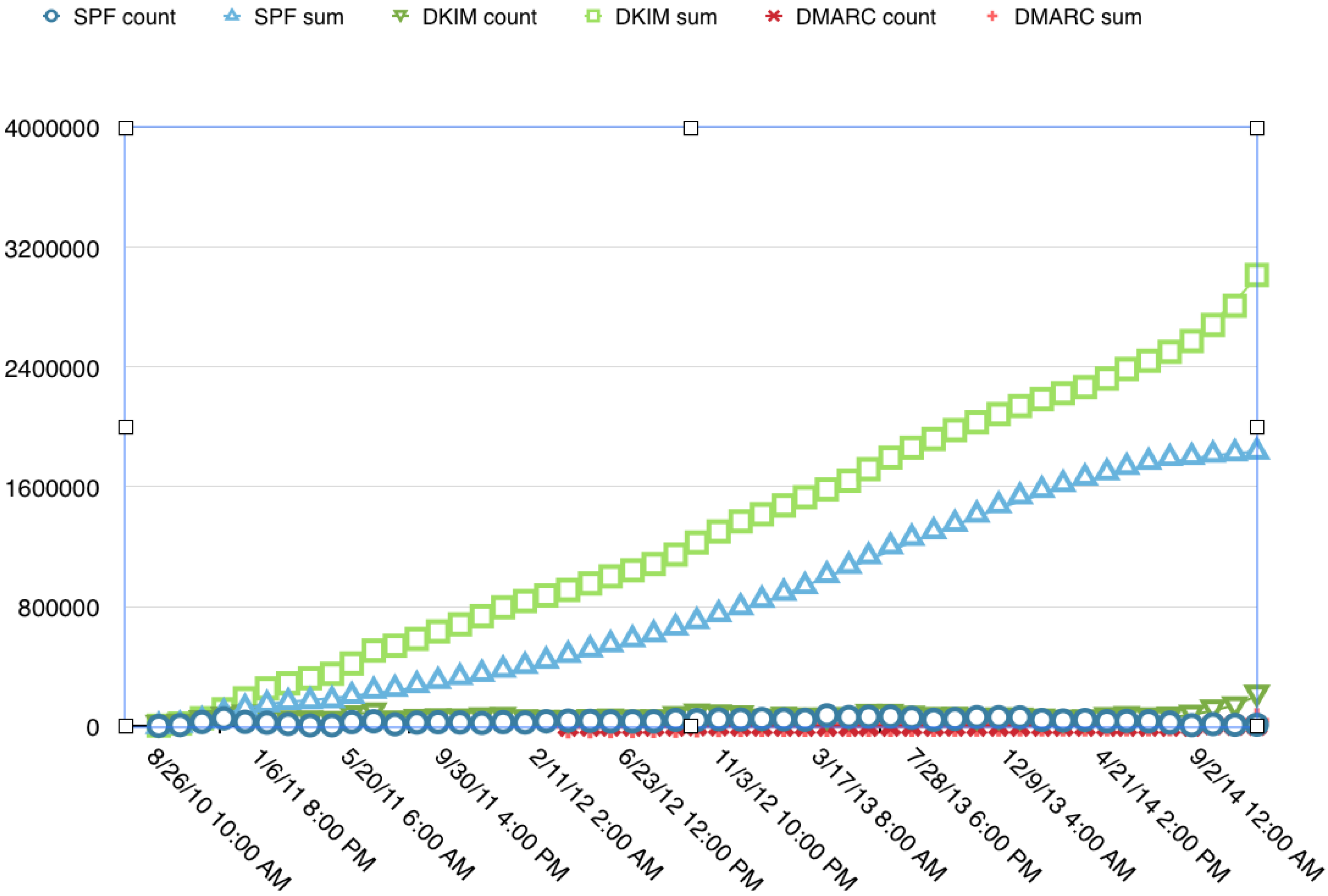
- Email clients that render known-to-be legitimate email in a different way..

- Email clients that automatically filter email based on identifier…. filter to where?

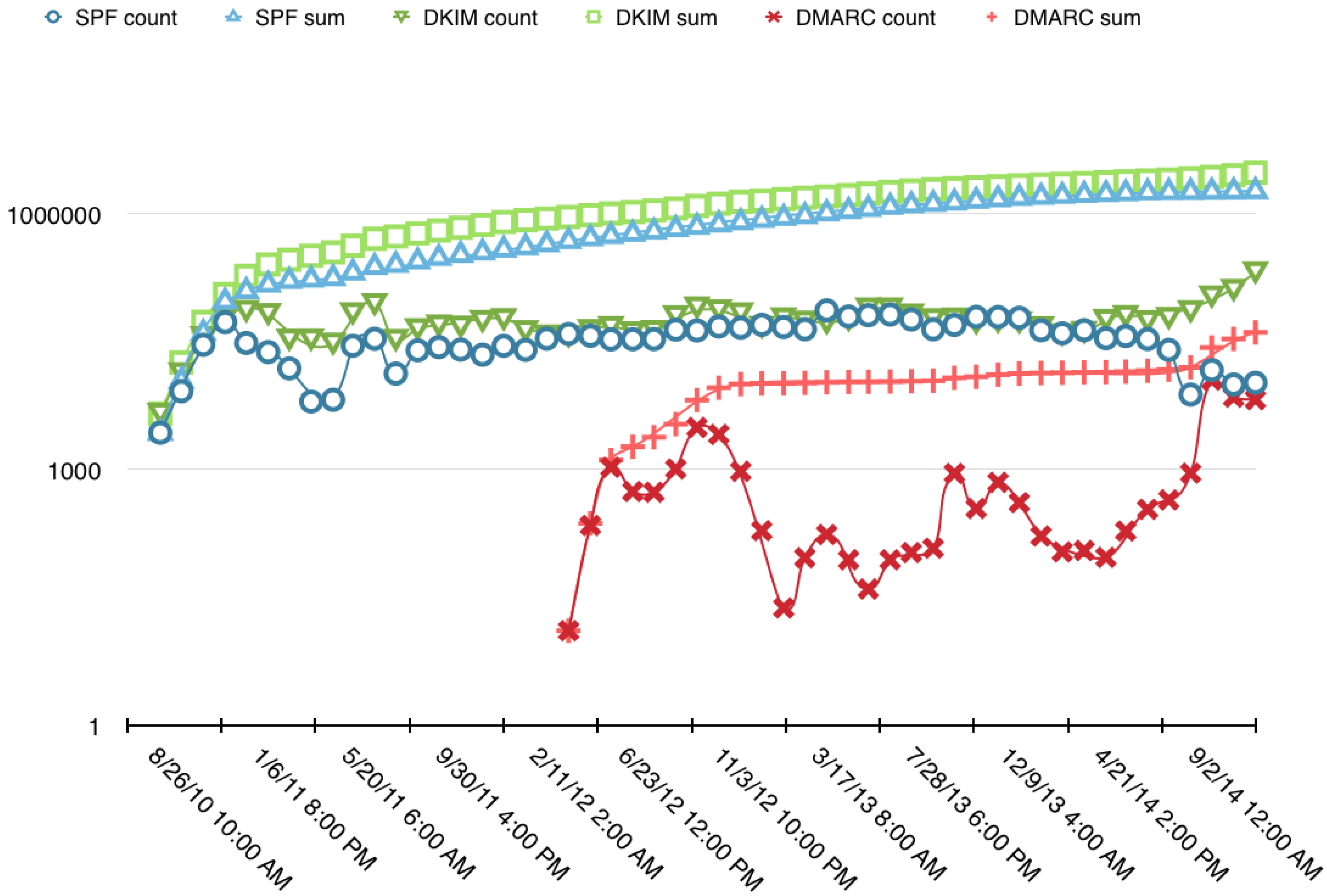
Measuring DMARC Adoption

- **By volume?** Facebook sends more email than anyone (by orders of magnitude).
- **By domain count?** German domain parker recently publish DMARC across “a few million” domains. (causing about 2x reports to be generated by reporters)
- **By report generators?** dmarcian.com/dmarc-status
- **By recording requests for DMARC records?**

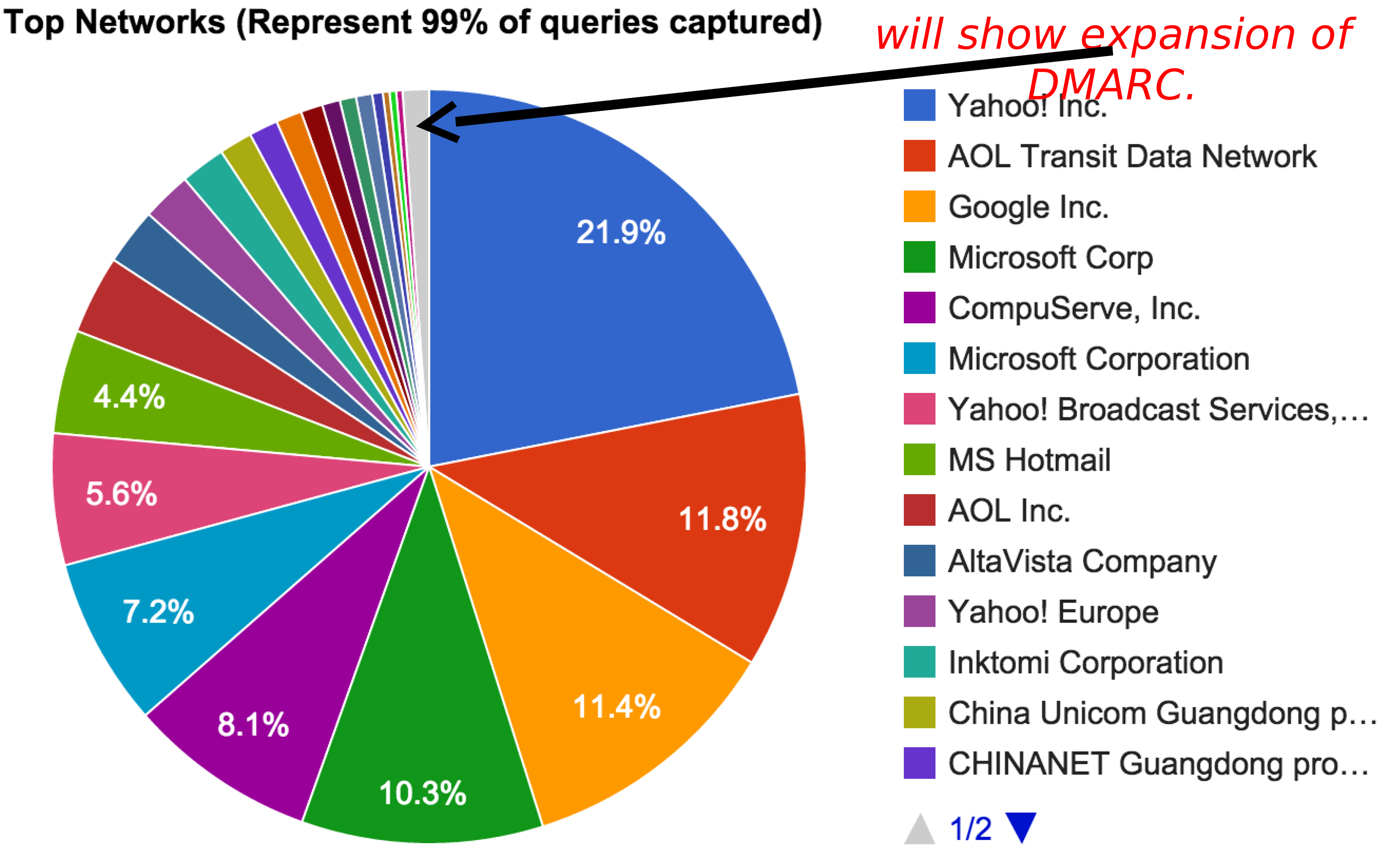
Authentication Timelines



Authentication Timelines

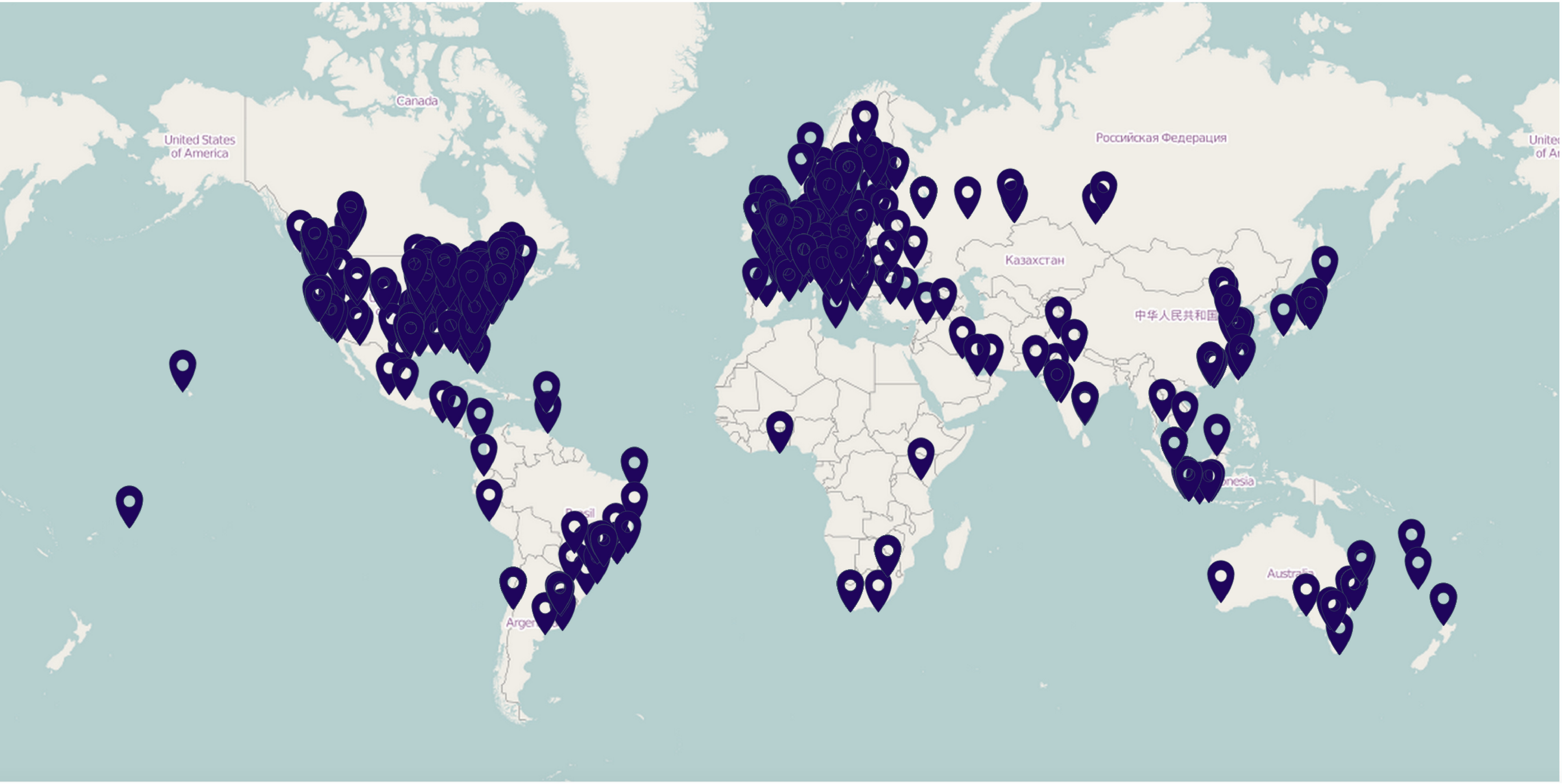


DMARC from DNS PoV: Today's Picture

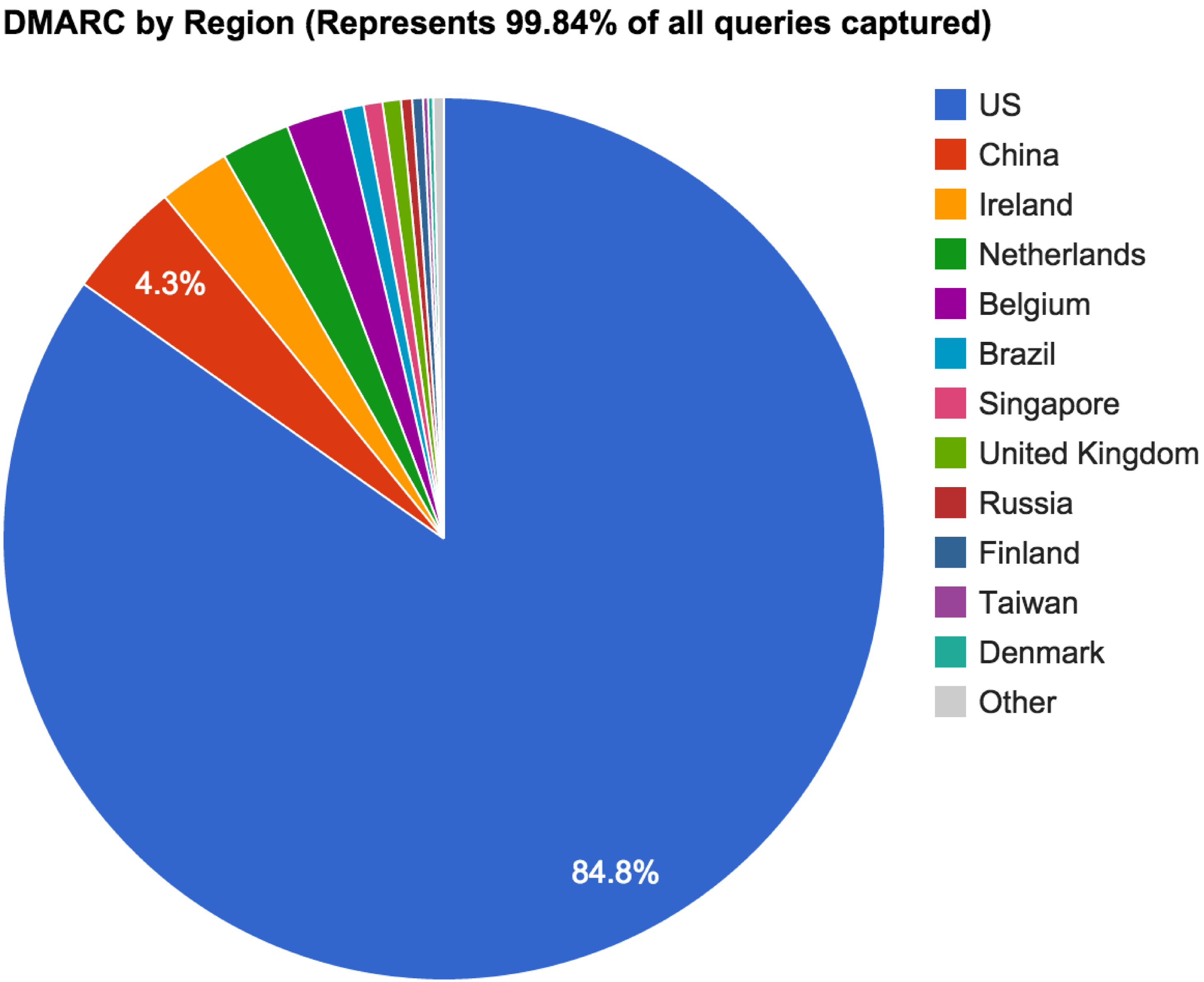


Note: The tail of this data will show expansion of DMARC.

DMARC from DNS PoV: Global Expansion



DMARC from DNS PoV: by Region



Getting it done..

Notes on dmarc deployment

How to Approach Deployment 1/2

- Just another project to manage
- Scope: deploy DMARC across all domains
  - *even the ones that do not send email*
- Deliverables:
  - Domain Catalog
  - DMARC records for all domains
  - Internal/partner comms around use of DMARC
  - Remediation training/plans to maintain DMARC

*Highly valuable regardless of DMARC

How to Approach Deployment 2/2

- Milestones:
  - Domain Management/Catalog Function*
  - DMARC records published for all domains
  - Analysis to show all partners/infrastructure/vendors sending on behalf of org
  - Remediation plan
  - Internal/partner communication resources
  - Integration into Operations
- Project installs process and then ends

Project Lessons

- Avoid deploying “one domain at a time”. Wasteful and will annoy everyone at org.

- Be ready to win company-wide buy in:
  - Security people don’t care about Delivery.
  - Marketing people don’t care about anti-phishing.
  - IT people don’t care to take on YA Project.
  - Executives **should** care about reducing exposure through compliance, right?

Project R.O.I.

- Greater return (and less investment) if DMARC across all domains (and not ad hoc).
- For all domains:
  - Anti-Fraud ROI
  - Simplified Delivery ROI
  - Domain Management Function ROI
  - Email Compliance ROI
- .. for something that will have to be done anyway as email evolves*

* if its not planned it’ll be ad hoc

ROI – Anti-Fraud

- ROI tied to intensity of domain abuse
- No abuse = zero return. Otherwise site-specific
- DMARC controls = less abuse means less cleanup (write offs, less support volume, etc)
- ½ of Brand Protection story
- Visibility into when attackers move on

ROI – Simplified Delivery

- ROI loosely tied to “email deliverability” issues
  - volume x complexity-of-domain = issues
- Significant chunk of deliverability spend goes away w/ DMARC
  - operational plumbing of email is simplified

- Quickly become a MUST to get email delivered.

ROI – Domain Mgmt Function

- ROI related to existing management process:
  - registering domains
  - tracking domain usage/ownership
  - managing domain controls & compliance
- Specific operational efficiency by creating DMF.
- Extend DMF to include SSL, DNS, etc.

ROI – Email Compliance

- Other ½ of Brand Protection. Is the brand consistent?
- Email domain policy now enforceable.
- Communicate with rest of world about posture of org’s email practice.
- Reduce exposure to various forms of liability.
- Ready to take advantage of new email developments.

Project R.O.I. Summary

- Lots of different ways to view ROI:
  - Anti-Fraud ROI
  - Simplified Delivery ROI
  - Domain Management Function ROI
  - Email Compliance ROI
- 1 project, goodies for everyone.
- If you’re NOT doing DMARC, you’re competing with bad guys to not look like the bad guy.

Nuts and Bolts

- Some domains easy (parked domains)
  - Still have to verify that they’re not in use.
- Some domains hard (top-level domain that is used for everything)
  - Have to disentangle usage. **This is where the real work happens.**
- *Indirect Email Flows*.
  - Mailing lists and forwarding. Site-specific impact.

Parting Thoughts

- DMARC.ORG is alive and well.
- dmarcian.com for tools & expertise.
- dmarc.io is Creative Commons companion site to dmarcian.com – directory of sorts.

- Domain owners need to do <some quantity> of work to take advantage of DMARC.
  - IMHO, reducing that work is key to more adoption.